



# UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/066,070	02/01/2002	Satyendra Yadav	10559-754001	2485
20985	7590	07/26/2005	EXAMINER	
FISH & RICHARDSON, PC 12390 EL CAMINO REAL SAN DIEGO, CA 92130-2081			HA, LEYNNA A	
			ART UNIT	PAPER NUMBER
			2135	

DATE MAILED: 07/26/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/066,070

Applicant(s)

YADAV, SATYENDRA

Examiner

LEYNNA T. HA

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on \_\_\_\_.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-30 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-30 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date 2/1/02.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_.

**DETAILED ACTION**

1. Claims 1-30 is pending.

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. **Claims 1-30 are rejected under 35 U.S.C. 102(b) as being anticipated by Trostle (US 5,919,257).**

**As per claim 1:**

Trostle discloses a machine-implemented method comprising:

examining a set of instructions embodying an invoked application to identify the invoked application; **[COL.2, lines 50-51 and COL.5, lines 22-23]**

obtaining an application-specific intrusion detection signature; and **[COL.5, lines 28-35]**

monitoring network communications for the invoked application using the application-specific intrusion detection signature to detect an intrusion. **[COL.5, lines 36-42 and COL.6, lines 13-17]**

Art Unit: 2135

**As per claim 2:** See col.3, lines 19-30; discussing tracking one or more characteristics of the network communications to identify application-specific abnormal communication behavior.

**As per claim 3:** See col.5, lines 50-52; discussing tracking one or more characteristics of the network communications comprises comparing the one or more characteristics with one or more configurable thresholds.

**As per claim 4:** See col.1 line 66 – col., line 3; discussing at least one of the one or more configurable thresholds comprises a threshold set by monitoring communications for the invoked application during a defined time window.

**As per claim 5:** See col.1, lines 39-41; discussing monitoring network communications comprises monitoring network communications in a network intrusion detection system component invoked with the invoked application.

**As per claim 6:** See col.4, lines 32-35; discussing the network intrusion detection system component and the invoked application run within a single execution context.

**As per claim 7:** See col.3, lines 8-30 and col.6, lines 13-17; discussing providing a first application-specific remedy for a detected intrusion; and providing a second application-specific remedy for identified application-specific abnormal communication behavior.

Art Unit: 2135

**As per claim 8: See col.2, line 66 – col.3, line 2 and col.6, lines 37-38;** discussing providing a first application-specific remedy comprises cutting at least a portion of the network communications for the invoked application, and wherein providing a second application-specific remedy comprises notifying a system administrator of the identified application-specific abnormal communication behavior.

**As per claim 9: See col.5, lines 44-45;** discussing obtaining the application-specific intrusion detection signature comprises loading the application-specific intrusion detection signature from a local signature repository.

**As per claim 10: See col.5, lines 44-45 and col.6, lines 13-20;** discussing obtaining the application-specific intrusion detection signature comprises: requesting the application-specific intrusion detection signature from a local signature repository in communication with a remote signature repository; and receiving the application-specific intrusion detection signature from the local signature repository.

**As per claim 11: See col.2, lines 44-60;** discussing the set of instructions reside in a file, and wherein examining the set of instructions comprises: applying a hash function to data in the file to generate a condensed representation of the data; and comparing the condensed representation with existing condensed representations for known applications.

Art Unit: 2135

**As per claim 12:**

Trostle teaches a machine-readable medium embodying machine instructions for causing one or more machines to perform operations comprising:

examining a set of instructions embodying an invoked application to identify the invoked application; **[COL.2, lines 50-51 and COL.5, lines 22-23]**

obtaining an application-specific intrusion detection signature; and **[COL.5, lines 28-35]**

monitoring network communications for the invoked application using the application-specific intrusion detection signature to detect an intrusion. **[COL.5, lines 36-42 and COL.6, lines 13-17]**

**As per claim 13: See col.3, lines 19-30;** discussing the operations further comprise tracking one or more characteristics of the network communications to identify application-specific abnormal communication behavior.

**As per claim 14: See col.1, lines 39-41;** discussing monitoring network communications comprises monitoring network communications in a network intrusion detection system component invoked with the invoked application.

**As per claim 15: See col.4, lines 32-35;** discussing the network intrusion detection system component and the invoked application run within a single execution context.

Art Unit: 2135

**As per claim 16: See col.3, lines 8-30 and col.6, lines 13-17;**

discussing the operations further comprise: providing a first application-specific remedy for a detected intrusion; and providing a second application-specific remedy for identified abnormal communication behavior.

**As per claim 17: See col.6, lines 37-38;** discussing the first and second application-specific remedies each comprise cutting at least a portion of the network communications for the invoked application.

**As per claim 18: See col.5, lines 44-45 and col.6, lines 13-20;** discusses obtaining the application-specific intrusion detection signature comprises: requesting the application-specific intrusion detection signature from a signature repository; and receiving the application-specific intrusion detection signature from the signature repository.

**As per claim 19: See col.5, lines 44-45 and col.6, lines 13-20;** discussing the signature repository comprises a local signature repository in communication with a remote signature repository.

**As per claim 20: See col.2, lines 44-60;** discussing examining the set of instructions comprises: applying a hash function to the set of instructions to generate a condensed representation; and comparing the condensed representation with existing condensed representations for known applications.

Art Unit: 2135

**As per claim 21:**

A system comprising:

a network; **[COL.3, lines 55-56]**

a security operation center coupled with the network; and **[COL.2, line 5 – COL.3, line 1 and COL.5, lines 47-48]**

one or more machines coupled with the network, each machine comprising a communication interface and a memory **[COL.4, lines 8-13]** including an execution area configured to perform operations comprising examining a set of instructions embodying an invoked application to identify the invoked application **[COL.2, lines 50-51 and COL.5, lines 22-23]**, obtaining application-specific intrusion criteria **[COL.5, lines 28-35]**, and monitoring network communications for the invoked application using the application-specific intrusion criteria to detect an intrusion **[COL.5, lines 36-42 and COL.6, lines 13-17]**.

**As per claim 22: See col.6, lines 34-35;** discussing the application-specific intrusion criteria comprises a normal communication behavior threshold.

**As per claim 23: See col.5, lines 28-35;** discussing the application-specific intrusion criteria comprises an intrusion signature.

**As per claim 24: See col.1, lines 39-41;** discussing monitoring network communications comprises monitoring network communications in a network intrusion detection system component running in an execution context with the invoked application.



Art Unit: 2135

**As per claim 25: See col.3, lines 8-30 and col.6, lines 13-17;**

discussing the operations further comprise providing an application-specific remedy for a detected intrusion.

**As per claim 26: See col.6, lines 37-38;** discussing providing an application-specific remedy comprises cutting at least a portion of the network communications for the invoked application.

**As per claim 27: See col.2, lines 39-59 and col.5, lines 40-45;** discloses requesting the application-specific intrusion criteria from the local repository; requesting the application-specific intrusion criteria from the master repository if the application-specific intrusion criteria is unavailable in the local repository; receiving the application-specific intrusion criteria from the master repository if requested; and receiving the application-specific intrusion criteria from the local repository.

**As per claim 28: See col.2, lines 44-60;** discussing examining the set of instructions comprises: applying a hash function to the set of instructions to generate a condensed representation; and comparing the condensed representation with existing condensed representations for known applications.

**As per claim 29:**

Trostle teaches a system comprising:

a security operation center; [COL.2, line 5 – COL.3, line 1 and COL.5, lines 47-48]

Art Unit: 2135

one or more machines **[COL.3, lines 55-59]**, each machine including means for identifying a process, obtaining a process-specific intrusion detection signature **[COL.5, lines 28-35]**, and monitoring network communications for the process using the process-specific intrusion detection signature to detect an intrusion; **[COL.5, lines 36-42 and COL.6, lines 13-17]**

and communication means coupling the one or more machines with the security operation center. **[COL.5, line 66 – COL.6, line 2 and lines 7-13]**

**As per claim 30: See col.3, lines 19-30;** discussing each machine further includes means for tracking one or more characteristics of the network communications to identify process-specific abnormal communication behavior.

### ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859.

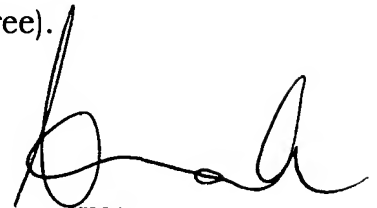
Art Unit: 2135

The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>.

Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

LHa



KIM VU  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER